FortiAuthenticator 3.0

What's New Guide

FortiAuthenticator 3.0 What's New Guide

October 22, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2013-10-22	Initial Release.

Introduction

This document lists and describes many of the new features added to FortiAuthenticator v3.0. For a complete list of all new FortiAuthenticator v3.0 features, please see the latest release notes.

This document, and all of the FortiAuthenticator v3.0 documentation, will continue to improve as we see the new features in action and as we get feedback about these documents from you. You can send comments and suggestions for improvements for all FortiAuthenticator 3.0 documents to techdoc@fortinet.com.

What's New

FortiAuthenticator v3.0 is a major feature release and includes new features in all functional areas of the product. There is a particular focus on enhancement of the Fortinet Single Sign-On (FSSO) feature set.

System features

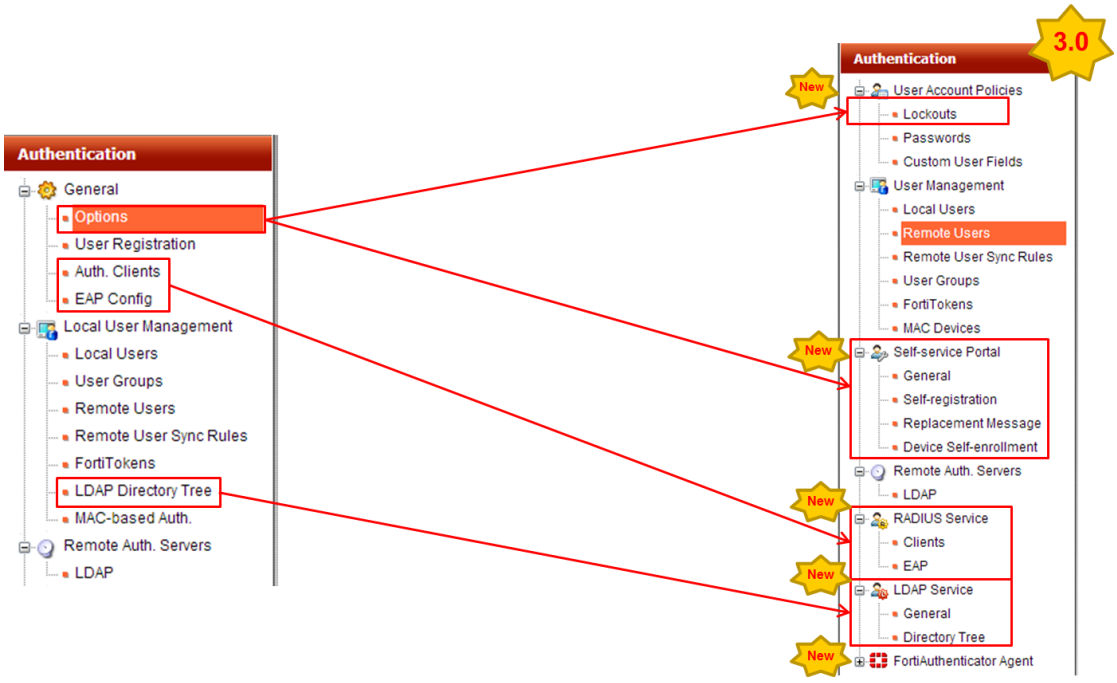
These are features related to general system operation and not a specific functional area.

GUI Reorganization

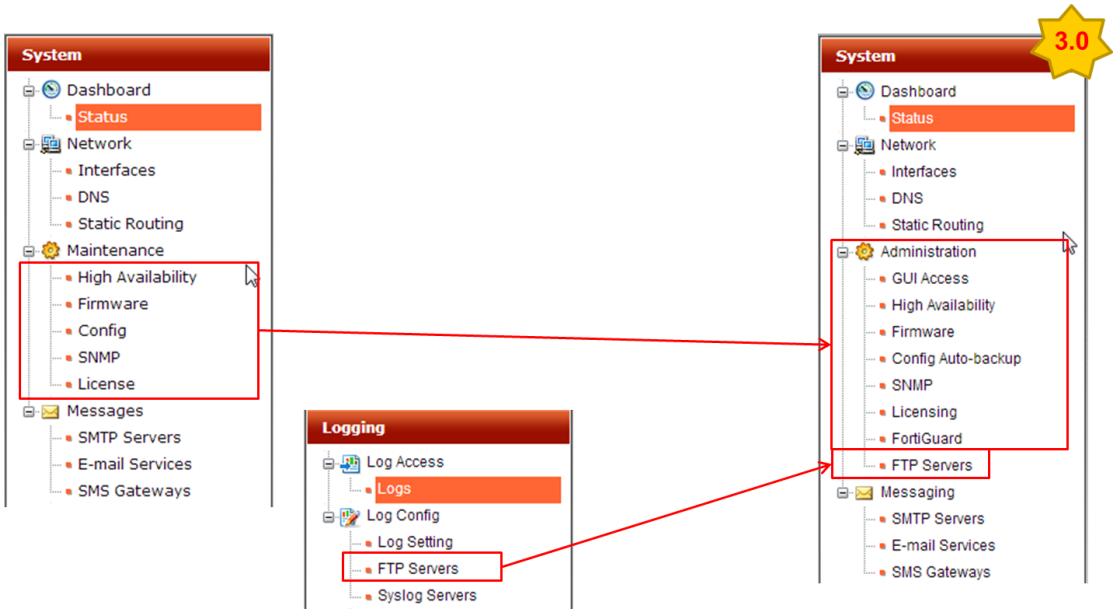
To reflect the wide range of changes which have been made in this and recent releases of FortiAuthenticator, and to incorporate new changes, the GUI has been reorganized to improve clarity and usability.

RADIUS features were previously configured as part of the General configuration, however, this generated the incorrect assumption RADIUS was not support. To make this clear, a new RADIUS Service option has been created where NAS Clients and EAP configuration can be configured,

Configuration of the self-service portal features has been given a dedicated tab covering all settings.



Maintenance has been renamed Administration to reflect the new features which have been added. FTP Settings have been moved to the System as they are no longer only used for log backup.



Multilingual support for user interface

Support has been added for language customization of various elements of the user facing GUI and SMS/E-mail messages. The following languages will be supported out of the box:

- Chinese (Traditional & Simplified)
- English
- French
- German
- Japanese
- Portuguese
- Russian
- Spanish

The GUI has 3 methods in which languages will be applied:

- Detect browser language setting and adjust display language as appropriate
- Administrator override for default
- Default system language

Customers will be able to generate and upload their own localized language files. Contact Fortinet Support should you required the translation pack. Customer generated language files can be submitted for inclusion in future official releases.

Scheduled config backup to FTP/SFTP

Schedule a regular backup of configuration from FortiAuthenticator to an external FTP or SFTP server. Primary and secondary servers are supported.

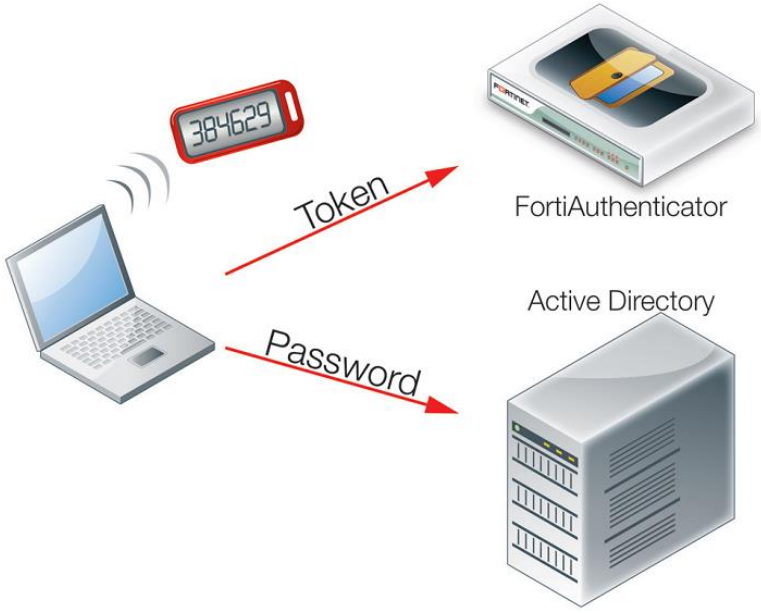
Authentication

Authentication covers all of the explicit authentication options within the FortiAuthenticator including RADIUS, LDAP, Two-Factor, EAP, guest management and user self-service features.

FortiAuthenticator Agent for Microsoft Windows

FortiAuthenticator supports two factor authentication via methods such as RADIUS and LDAP. It is not possible to replace the authentication process for Microsoft Windows Domain authentication so Fortinet have introduced a Two Factor Authentication Plugin Module to enhance the existing domain login process. FortiAuthenticator Agent for Microsoft Windows utilizes the Credential Provider Plugin system provided by Microsoft to add validation of a Token Passcode to the standard username and password authentication process.

This Agent allows the Username and Password to be validated directly via Active Directory as usual whilst the Token Passcode is validated via a HTTPS connection to the FortiAuthenticator.



FortiAuthenticator Agent for Microsoft Windows supports a range of features including:

- Fail open / closed if connection to FortiAuthenticator is unavailable
- Administrator override
- Login with administrators One-Time Passcode
- Exempted accounts
- Support for password change
- CLI based configuration to simplify GPO roll out
- Limit domains for which One-Time Passcode is required

Table 1: Supported Operating Systems

Server Operating Systems	Desktop Operating Systems
Windows Server 2008 DataCenter X86	Windows Vista Ultimate X86
Windows Server 2008 Enterprise X64	Windows Vista Business X64
Windows Server 2008 R2 DataCenter X64	Windows Vista Enterprise X64
Windows Server 2008 R2 Enterprise X64	Windows 7 Professional X86
Windows Server 2012 Standard X64	Windows 7 Ultimate X64
Windows Server 2012 DataCenter X64	Windows 7 Enterprise X64
	Windows 8 Professional X64
	Windows 8 Enterprise X64

Microsoft Windows 8 x86 standard is unsupported as it is cannot be connected to the domain.

Microsoft Windows XP has not been supported due to its imminent end of support with Microsoft. Please contact your Fortinet Account Manager is this is an issue.

Replacement Token Workflow

A token replacement workflow has been introduced to allow a token to be temporarily replaced if forgotten or lost. A temporary SMS or email token can be assigned to the user until the primary token has been replaced.

User Expiration Enhancements

In previous releases, user account expiry could only be set for users registering via the self-registration portal and once set, this could not be modified. The ability to configure and modify user account expiry has been extended to the user management interface

User Lockout Enhancements

Two new enhancements to the user lockout facility have been implemented:

- Permanent lockout on multiple failed attempts. Extends existing temporary lockout feature by requiring administrator unlock.
- Lock out on user inactivity. Monitor for unused accounts to allow recovery of dormant accounts.

Guest portal enhancements

The FortiAuthenticator guest self-registration portal allows service providers to allow open access to networks such as free WiFi in hotels or shops, on the basis that the user first has to register. This registration can either be accepted automatically and the user provided with login credentials, or can be sent to an administrator for approval.

With FortiAuthenticator 3.0, a range of new features have been added to allow customisation of the registration portal:

- Ability to remove the requirement for Username and use mobile number provided
  - Allows the login credentials to be SMSed to user which is a guarantee of identity for compliance purposes.
- Customization of the fields which are displayed on the self-registration page
  - Allows organizations to tailor the information collected from their customers based on business needs
- Customizable HTML for self-registration page
  - HTML can be fully customised to match corporate look and feel and to add custom messages.
  - Images and content/frames/adverts can be pulled in from external sources.
  - Images can be uploaded and directly served from the FortiAuthenticator.

Replacement Messages

The concept of replacement messages has been added, allowing the administrator full control of the content displayed to the end user in a variety of interfaces including:

- E-mail Token Message
- E-mail Token Subject
- User Registration Receipt Message (via e-mail or browser)
- User Registration Receipt Message (via SMS)
- Login Page
- Token Login Page
- Password Reset Complete Page
- Password Reset E-mail Instruction Page
- Password Set Complete Page
- User Registration Confirmation Page (with Admin Approval)

- SMS Verification Page
- User Registration Confirmation Page
- Resend Registration Receipt Page
- SMS One-Time Passcode Message
- User Registration Page

User device certificate self-enrolment

Certificate management has traditionally been complicated. FortiAuthenticator simplifies creation, signing, management and distribution of certificates via SCEP. FortiAuthenticator 3.0 further simplifies the user management process by introducing user device self-enrolment. This feature allows end-users to log into the FortiAuthenticator user portal and create certificates for their devices for use in, for example BYOD wireless authentication.

User self service certificate enrolment supported for specific devices using the following protocols and methodologies

- iPhone/iPad → Automated SCEP via Mobile Config
- Android → Manual PKCS#12
- Windows → PKCS#10 CSR
- Other → SCEP, PKCS#10 CSR, Manual PKCS#12

User Management API

To enable integration of the FortiAuthenticator with third party portals and other systems, the API has been extended to enable programmatic user management including:

- Creation and deletion of users
- Creation and deletion of groups
- Assignment of users to groups

Apply Complexity Settings on Randomly Generated Passwords

Auto-generated passwords have previously been overly complicated, making login using mobile devices difficult. The ability to enforce password complexity has been implemented to allow the administration control which character combination is used in the generation of random passwords.

Self-registration user group

Ability to select a group in which to drop all self-registered users into following self-registration. This prevents self-registration users being accidentally included on other user policies on shared use systems.

Fortinet Single Sign On

Fortinet Single Sign-On (FSSO) is a method used by FortiGate and FortiCache to transparently identify users on the network.

FortiAuthenticator uses both transparent and non-transparent methods to gather user login status information from a variety of disparate locations; consolidates and embellishes the information before supplying to FortiGate or FortiCache devices for use in identity based policies.

The previous methods of gathering user identity included:

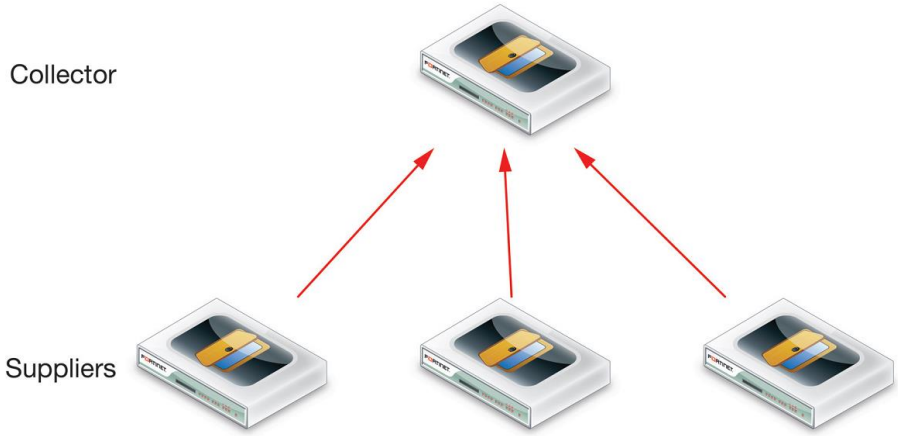
FortiAuthenticator Portal Login	(Manual Login)
FortiAuthenticator Portal Login with home page widgets	(Partially transparent)
FortiAuthenticator Single Sign On Mobility Agent	(Transparent)
Active Directory Polling	(Transparent)
RADIUS Accounting	(Transparent)

FortiAuthenticator 3.0 introduces a range of new FSSO functionality.

Hierarchical tiering for DC polling

Tiering of collectors and supplier s allows for the large scale deployment of regional systems performing detection of user identification, local LDAP group lookup and distribution of events to top level collectors which distribute login events to FortiGate and FortiCache devices.

Figure 1: Tiering collectors and suppliers

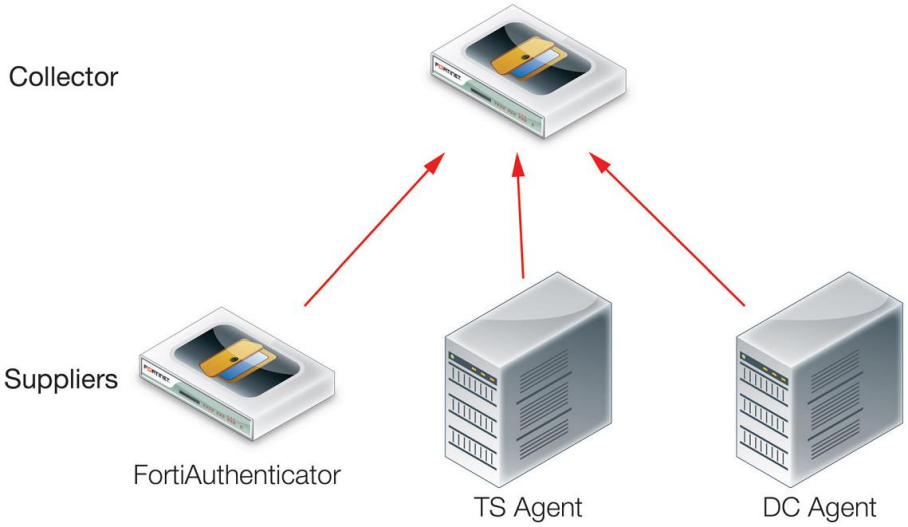


Support DC and TS agents

FortiGate support the concept of DCAgent software for collection of login information from Windows Active Directory systems via polling or installation on the domain controller. TSAgent is a similar concept but collects user login information from Citrix or Windows Terminal Servers.

FortiAuthenticator implements the polling functionality directly, however, it also accepts a feed from DCAgent and TSAgent installations if necessary.

Figure 2: DC and TS agents



FSSO Exclude Users

Service accounts (AV and other software) in a Microsoft Windows environment can cause "ghost" logins overwriting valid login. Exclusions allow such service accounts to be ignored to avoid this issue.

FSSO Workstation Logoff detection

Whilst detection methods such as Active directory polling can identify user login events, they are unable to directly detect user logoff. FSSO workstation logoff detection utilises the WMI protocol to detect if the user is still logged in to the workstation, if not, the login is removed.

- Supports DC Polling, SSO Mobility, DC and TS Agents (currently not RADIUS Accounting or Portal)

FSSO Concurrent User Limit

To facilitate a flexible BYOD policy, FortiAuthenticator 3.0 introduces the ability to restrict the number concurrent devices a single user account can have logged in.

FSSO user licensing has been modified to support this feature.

Version 2.2 and below: 6 users	
User1	192.168.0.1
User1	192.168.0.2
User1	192.168.0.3
User2	192.168.0.4
User2	192.168.0.5
User3	192.168.0.6

Version 3.0 and above: 3 users	
User1	192.168.0.1
	192.168.0.2
	192.168.0.3
User2	192.168.0.4
	192.168.0.5
User3	192.168.0.6

API FSSO Login

The FortiAuthenticator API has been extended to allow third party systems push login/logout events into the FSSO database. This allows the integration of third party authentication applications and web portals with Fortinet Single Sign-On.